

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039082

(43)Date of publication of application : 12.02.1999

(51)Int.Cl.

G06F 3/02  
 G06F 1/00  
 H04L 9/08  
 H04L 9/10  
 H04L 9/32  
 H04L 9/36

(21)Application number : 09-190065

(71)Applicant : FUJITSU LTD

(22)Date of filing : 15.07.1997

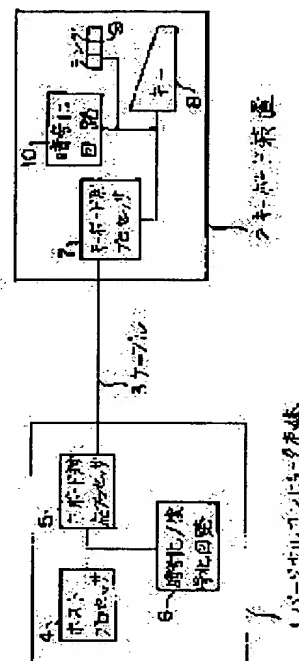
(72)Inventor : HIGUCHI TAIHO

(54) KEYBOARD DEVICE HAVING SECURITY FUNCTION AND METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a keyboard device having a high security function.

SOLUTION: A ciphering/decoding circuit 6 and a ciphering circuit 10 are provided for a main body 1 and the keyboard device 2. The keyboard device 2 waits for the input of user ID and a password from a key 8 with the power supply of the main body 1. When a user ID is inputted and it is transmitted to the main body 1, random numbers for message-compressing the password are transmitted from the main body 1 to the keyboard device 2. The keyboard device 2 message-compresses the password by the random numbers and transmits it to the main body 1. The main body 1 compares the password which is transmitted and message-compressed with the password which is message-compressed inside and certifies a user. An open key is transferred to the keyboard device 2 and a cipher key used for session is transmitted from the keyboard device 2 to the main body 1. Then, session is executed by using the open key hereafter.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-39082

(43) 公開日 平成11年(1999) 2月12日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 0 6 F 3/02

3 8 0

G 0 6 F 3/02

3 8 0 B

1/00

3 7 0

1/00

3 7 0 E

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

9/10

6 0 1 E

9/32

6 2 1 A

審査請求 未請求 請求項の数16 O L (全 11 頁) 最終頁に続く

(21) 出願番号

特願平9-190065

(22) 出願日

平成9年(1997) 7月15日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 樋口 大奉

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74) 代理人 弁理士 大昔 義之 (外1名)

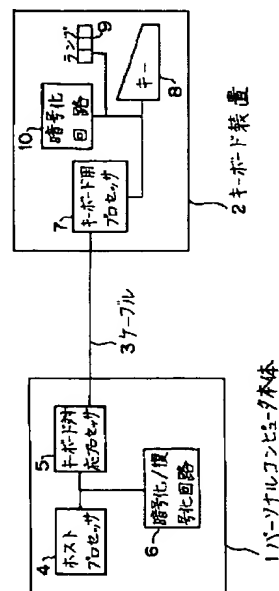
(54) 【発明の名称】 機密保持機能を有するキーボード装置及びその方法

(57) 【要約】

【課題】機密保持機能の高いキーボード装置を提供することである。

【解決手段】本体1とキーボード装置2に暗号化／復号化回路6及び暗号化回路10を設ける。本体1の電源投入によりキーボード装置2は、キー8からのユーザID及びパスワードの入力待ちとなる。ユーザIDが入力され、本体1へ送信されると、今度は本体1からパスワードをメッセージ圧縮するための乱数がキーボード装置2に送られ、キーボード装置2はパスワードを乱数によってメッセージ圧縮して本体1へ送信する。本体1では、送信されてきたメッセージ圧縮されたパスワードと内部でメッセージ圧縮したパスワードとを比較し、利用者の認証を行う。次に、キーボード装置2に公開鍵が渡され、キーボード装置2からセッションに使う暗号鍵が本体1に送信される。そして、以後、この暗号鍵を用いてセッションを行う。

本発明のキーボード装置の第1の実施形態の構成を示す図



## 【特許請求の範囲】

【請求項 1】コンピュータ装置の本体に接続されて用いられるキーボード装置であって、前記本体に送出する信号を暗号化する暗号化手段と、暗号化された前記信号を送出する送出手段とを備えることを特徴とするキーボード装置。

【請求項 2】前記本体の電源投入後に、前記本体に対して利用者のパスワードを暗号化して送信することを特徴とする請求項 1 に記載のキーボード装置。

【請求項 3】前記パスワードを入力した前記利用者が前記本体において正当な利用資格者と認証された場合に、前記本体へ送信する信号の送信を暗号化して行うための暗号鍵を前記本体に送信することを特徴とする請求項 2 に記載のキーボード装置。

【請求項 4】前記暗号鍵は前記本体から送信されてきた公開鍵に基づいて暗号化して前記本体に送信することを特徴とする請求項 3 に記載のキーボード装置。

【請求項 5】前記キーボード装置に何の入力も無い場合にも、ダミーデータを暗号化して、前記本体に対して定常的に送出することを特徴とする請求項 1 に記載のキーボード装置。

【請求項 6】前記本体に送出する信号の少なくとも一部を光信号に変換して、前記本体に送出することを特徴とする請求項 1 に記載のキーボード装置。

【請求項 7】前記キーボード装置の操作者が所定の時間入力を行わないことにより前記信号を暗号化することを中止することを特徴とする請求項 1 に記載のキーボード装置。

【請求項 8】前記キーボード装置に設けられるキーボード用プロセッサと前記暗号化手段とを一体化して、容易に分解できないように封入したことを特徴とする請求項 1 に記載のキーボード装置。

【請求項 9】前記本体側よりの指示により、前記信号を暗号化しない通常の動作モードと、前記信号を暗号化する暗号化モードの切り換え可能に構成され、暗号化モードに入ったことを示す特有の表示を行うことを特徴とする請求項 1 に記載のキーボード装置。

【請求項 10】コンピュータ装置の本体に接続されて用いられるキーボード装置と前記本体との間の通信の機密を保持する方法であって、前記本体に送出する信号を暗号化するステップと、暗号化された前記信号を送出するステップとを備えることを特徴とするコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 11】前記本体の電源投入後に、前記本体に対して前記コンピュータ装置の利用者のパスワードを暗号化して送信することを特徴とする請求項 10 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 12】前記パスワードを入力した前記利用者が

前記本体において正当な利用資格者と認証された場合に、前記本体へ送信する信号の送信を暗号化して行うための暗号鍵を前記本体に送信することを特徴とする請求項 11 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 13】前記暗号鍵は前記本体から送信されてきた公開鍵に基づいて暗号化して前記本体に送信することを特徴とする請求項 12 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 14】前記キーボード装置に何の入力も無い場合にも、ダミーデータを暗号化して、前記本体に対して定常的に送出することを特徴とする請求項 10 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 15】前記本体に送出する信号の少なくとも一部を光信号に変換して、前記本体に送出することを特徴とする請求項 10 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項 16】前記キーボード装置の操作者が所定の時間入力を行わないことにより前記信号を暗号化することを中止することを特徴とする請求項 10 に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機密保持機能を有するキーボード装置、及びコンピュータ本体とキーボード装置間の通信の機密保持方法に関する。

【0002】

【従来の技術】コンピュータによる犯罪の可能性が指摘されてから、データの保全と利用者の特定のために多くの保護手段が用いられるようになった。これには暗号化やパスワードによる利用者の特定などがある。

【0003】しかし、その反面で最もポピュラーな入力手段であるキーボード装置については安全性が極めて低いのが現状である。特に、デスクトップタイプの分離型のキーボード装置は標準化が行われ、低コストである反面で安全性についてはほとんど考慮されていない。長いケーブルで比較的の高いレベルの信号を扱っていることで、ここを流れる信号は容易に外部で拾い出して復元することができる。またキーボード本体も容易に分解可能な構造であり、操作性からある程度の大きさを必要としながら軽量化されているために内部は空洞状態で盗聴器（キーボード装置のキーから入力される信号を外部から取得する装置を盗聴器と読んでおり、以降、このような外部からの信号の取得を盗聴という）を配置することも容易である。

【0004】図 7 は、従来のキーボード装置及びパーソナルコンピュータ本体の構成の一例を示す図である。71 は、パーソナルコンピュータ本体であり、表示装置等

は図示されていないが通常のパーソナルコンピュータが備える表示装置等は備えているものとする。72はキーボード装置である。73は両者を接続するケーブルである。パーソナルコンピュータ本体71にはキーボード装置72からの信号を受け取るキーボード対応プロセッサ75があり、ここでキーボード装置72のキー77を押すことによって生成される符号（文字コード等）の変換とホストプロセッサ74へキーボード装置72から入力されたデータを送信するための割り込み等を行う。キーボード装置72にもキーボード用プロセッサ76が格納され、キーボード用プロセッサ76はキーボード装置72のキー77のどのキーが打鍵されたかを判断して、対応する符号の生成を行う。ケーブル73は、上りまたは下り（キーボード装置72からパーソナルコンピュータ本体71へ向かう方向を上りとしている）の信号を送出する信号線、クロック線、電源線等からなり、パーソナルコンピュータ本体71からのコマンド、キーボード装置72からの信号がシリアルに伝送される。キーボード装置72にはキー77及び大文字／数字などのモードを表示する、パーソナルコンピュータ本体71の制御により点灯／滅灯されるランプ78がある。キー77が打鍵されることによりその位置と同時に打鍵の情報がキーボード用プロセッサ76によって変換されてケーブル73を通してパーソナルコンピュータ本体71に送出される。

#### 【0005】

【発明が解決しようとする課題】従来、無資格者による操作の防止のために、キーボード装置をパスワードでロックすることは実施されてきた。これは、パーソナルコンピュータ本体側のキーボード装置からの符号（コード）を解読する専用プロセッサ（図7のキーボード対応プロセッサ75）内に所定の文字列を予め設定しておき、キーボード装置からこれに一致する文字列が入力されるまで、全ての入力を無視することにより無資格者の操作が行えないようにする方法である。

【0006】しかし、この場合にもパスワードなどの入力はキーボードから行われるので、このパスワードを表す信号が外部で収集可能であれば折角の保護手段も効果がなくなってしまう。

【0007】従って、ホテルや公共の場に配置されるパーソナルコンピュータが操作する資格の無い人に操作されたり、パスワードが盗まれたりする可能性がある。本発明の課題は、機密保持機能の高いキーボード装置を提供することである。

#### 【0008】

【課題を解決するための手段】本発明によるキーボード装置は、コンピュータ装置の本体に接続されて用いられるキーボード装置であって、前記本体に送出する信号を暗号化する暗号化手段と、暗号化された前記信号を送出する送出手段とを備えることを特徴とする。

【0009】また、本発明による機密保持方法は、コンピュータ装置の本体に接続されて用いられるキーボード装置と前記本体との間の通信の機密を保持する方法であって、前記本体に送出する信号を暗号化するステップと、暗号化された前記信号を送出するステップとを備えることを特徴とする。

【0010】上記本発明の構成によれば、コンピュータ装置の本体へキーボード装置から情報を送る場合に、暗号化して送るので、コンピュータ装置とキーボード装置とを接続するケーブルの部分で盗聴されても容易には情報を盗まれることがない。

【0011】また、コンピュータ装置が起動した状態で、すぐに、利用者にユーザIDとパスワードの入力を行うが、このパスワードも暗号化あるいはメッセージ圧縮してコンピュータ装置本体に送信するようにすることによって、パスワードそのものが盗聴されることを防ぐことができる。

【0012】このように、キーボード装置からコンピュータ装置本体に情報が送信される間のケーブルの部分での盗聴を困難にすることが出来るので、機密保持機能の高いキーボード装置を提供することができる。

#### 【0013】

【発明の実施の形態】図1は、本発明のキーボード装置の第1の実施形態の構成を示す図である。パーソナルコンピュータ本体1にはホストプロセッサ4及びキーボード対応プロセッサ5が従来の構成と同様に設けられているが、本実施形態においては、更に、暗号化／復号化回路6が設けられている。また、キーボード装置2は、従来の構成であるキーボード用プロセッサ7、キー8、及びランプ9を備えると共に、暗号化回路10を備えている。パーソナルコンピュータ本体1に設けられる暗号化／復号化回路6及びキーボード装置2に設けられる暗号化回路10は、パーソナルコンピュータ本体1とキーボード装置2との間でケーブル3を介して転送されるデータあるいは符号（文字コード）等を暗号化するためのものである。パーソナルコンピュータ本体1とキーボード装置2との間を転送される符号等を暗号化することにより、ケーブル3のどこかに盗聴装置が取り付けられていても、盗聴した者は、ケーブル3を転送されている符号がどのようなものか解読することが容易でないので、機密保持機能を高めることが出来る。

【0014】なお、パーソナルコンピュータ本体1のホストプロセッサ4は、パーソナルコンピュータの一般的な処理を行うプロセッサであり、アプリケーションの実行などを行う。キーボード対応プロセッサ5は、キーボード装置2から送られてくる符号を表す信号を意味のある文字コード等に変換してホストプロセッサ4に渡す役割をしており、ホストプロセッサ4とキーボード装置2とのインターフェースを行うものである。キーボード装置2のキーボード用プロセッサ7は、キー8で生成され

た信号を、パーソナルコンピュータ本体 1 のキーボード対応プロセッサ 5 が意味のある文字コード等に変換できるように符号に変換するインタフェースの役割を行うものである。ランプ 9 は、キー 8 の特殊キーを押下することによって入力モード等がどのような状態にあるかを示すもので、パーソナルコンピュータ本体 1 からの指示によりキーボード用プロセッサ 7 が制御するものである。例えば、ランプ 9 は大文字入力の場合に点灯させる。

【0015】本実施形態では、パスワードをキーボード装置 2 からパーソナルコンピュータ本体 1 に送信する場合にも、乱数を用いてパスワードをメッセージ圧縮して送信するようにするので、ケーブル 3 の途中で盗聴されても盗聴した者にはパスワードが分からないようになっている。この乱数はパーソナルコンピュータ本体 1 からキーボード装置 2 に送信され来たものを使う。この場合にも、キーボード装置 2 は、パスワードを乱数でメッセージ圧縮して送信し、パーソナルコンピュータ本体 2 は送信されてきたメッセージ圧縮されたパスワードと内部で圧縮したパスワードとを圧縮されたままの状態と比較する。

【0016】パスワードをキーボード装置 2 から入力すると、パーソナルコンピュータ本体 1 は以後にケーブル 3 を用いて転送される符号の暗号化のための鍵をキーボード装置 2 へ送信する。この暗号鍵を盗聴されては、機密保持機能が保てないので、暗号鍵も暗号化して送信するようにする。この暗号鍵を暗号化するための鍵は公開鍵を使用するようにする。すなわち、パーソナルコンピュータ本体 1 からキーボード装置 2 へ公開鍵を予め送信する様に。公開鍵は第三者が取得しても、事実上、その公開鍵で暗号化されたデータを解読することは不可能なので、ケーブル 3 の途中で盗聴されても問題は生じない。

【0017】公開鍵を使用して符号の暗号化に必要な暗号鍵をパーソナルコンピュータ本体 1 からキーボード装置 2 へ送信し、その後は、公開鍵を使って暗号化されて送信された暗号鍵に基づいて処理速度の速い暗号化方法を使って符号の転送を行う。暗号鍵が暗号化されて送信されるので、盗聴されても第三者にはパーソナルコンピュータ本体 1 とキーボード装置 2 との間の符号の転送の内容を知られることはない。

【0018】電源投入時のような場合、キーボード装置 2 はパスワードの投入待ち状態となる。これはパーソナルコンピュータ本体 1 からの指示により例えばランプ 9 を複数個同時に点滅させる等の手段で示される。ここで操作者が改行キーで終わる一連のパスワードを入力すると、パーソナルコンピュータ本体 1 より送信された乱数とこのパスワードを組み合わせて、例えば、MD 5 に基づくメッセージ圧縮を行い、その結果がパーソナルコンピュータ本体 1 に送出される。パーソナルコンピュータ本体 1 ではこの結果を内部の同様に圧縮されたパス

ワードと照合することで操作者が利用資格者であることを認識できる。次に、パーソナルコンピュータ本体 1 は固有の公開鍵をキーボード装置 2 に送出する。キーボード装置 2 はこの公開鍵により、このセッションに使用する暗号鍵をパーソナルコンピュータ本体 1 に送出し、これ以降はキーボード装置 2 からの送出データは全て暗号化してパーソナルコンピュータ本体 1 に送出する。この暗号化は利用者からのリセット指示、パーソナルコンピュータ本体 1 からのセッションの終了または一定時間入力がない等による切断により解除され、キーボード装置 2 は再びパスワードの入力待ちになる。これらの暗号化の解除はホストプロセッサ 4 の監視の下に行われる。

【0019】MD 5 はメッセージを所定のルールに従い圧縮する算法である。この圧縮結果を同じ圧縮方法で圧縮されたメッセージと比較することで元のメッセージとの同一性が高い確率で保障される。逆に圧縮前のデータの一部と圧縮結果から元のメッセージを復元することは困難である。このことから安全でない伝送手段を用いての認証の手段として用いられるものである。MD 5 の詳細については、インターネット・アーキテクチャ委員会が発行する標準勧告文書である以下の文書を参照されたい。「Network Working Group, Request for Comments: 1321, The MD5 Message-Digest Algorithm, R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992」

公開暗号鍵は、ここでは RSA 方式等の公開鍵を使用する。元来が一定期間の保護で十分なパスワード等の保護が目的であるから、暗号の強度すなわち鍵の長さはコスト・性能のトレードオフにより決定される。本実施形態では、パーソナルコンピュータ本体 1 側が秘密鍵を持ち、キーボード装置 2 に対して公開鍵を送出する。公開鍵であるので仮に傍受されても問題は発生しない。キーボード装置 2 のコストを下げるために、例えば、秘密鍵とモジュロ数は 512 ビット相当、公開鍵は 32 ビット相当などの値が選ぶのが好ましい。

【0020】図 2 は、本実施形態のキーボード装置の構成の一例を示す図である。図 1 にも示したように、キーボード装置はキー 8、キーボード CPU (キーボード用プロセッサ) 7、及び暗号化回路 10 からなる。キー 8 には、「a」、「b」、「c」等の各記号を表すキーが複数配列されており、各キーにはそのキーが存在する位置を X 座標と Y 座標で表すための配線 20、21 がなされている。キー 8 のいずれか 1 つのキーが押されると、この配線 20、21 に信号が流れ、キーボード CPU 7 に、押下されたキーの X 座標位置と Y 座標位置を入力するようになっている。

【0021】キーボード CPU 7 は、この X 座標位置と Y 座標位置の入力を受けて、押下されたキーに対応する記号が何かを演算し、パーソナルコンピュータ本体 1 に送信するための符号を生成する。更に、本実施形態で

は、キーボードCPU7が生成した符号を暗号化回路10で暗号化して、キーボードCPU7に返して、ケーブル3を介してパーソナルコンピュータ本体1に送出する。

【0022】暗号化回路10がキーボードCPU7で生成された符号を暗号化する場合に、使用する暗号鍵は、前述したように、公開鍵を用いてパーソナルコンピュータ本体1に送信された暗号鍵であり、暗号化回路10に組み込まれているものである。前述したように、キーボード装置2は、標準化および軽量化が図られていて、安価であるが、簡単に分解可能な構成となっている。したがって、暗号化回路10が符号の暗号化に使う暗号鍵を盗もうとすれば、キーボード装置2を分解して、中にある暗号化回路10を解析すれば、暗号鍵を盗むことが出来る。このように、キーボード装置2内に暗号化回路10を設けただけでは、機密保持機能は万全ではない。

【0023】そこで、本実施形態では、キーボードCPU7と暗号化回路10とを樹脂などで固めるなどして、パッケージ化する。このようにすれば、暗号化回路10を容易には取り外すことができなくなると共に、暗号化回路10を調べることが難しくなるので暗号化回路10から暗号鍵が盗まれる可能性を小さくすることができ

る。

【0024】すなわち、従来用いられているキーボードのX、Y座標の位置情報をキーボードCPU7がどう利用しているかは外部からは観測されないもので、この限りでは安全である。しかし、本実施形態によるキーボードCPU7と暗号化回路10の間の配線はキー8の押下に対応する符号などクリティカルな信号が流されるので外部に漏洩しない措置が必要である。そこで、例えば、両者を一個のパッケージに封入したり、金属箔で覆って樹脂等で容易に剥がれないようにするのである。

【0025】図3は、本実施形態の一連の処理フローを表すタイムチャートである。まず、電源が入れられシステムが立ち上がると、パーソナルコンピュータ本体1からキーボード装置2へ、暗号モード移行指示が出される。暗号モードとは、パーソナルコンピュータ本体1とキーボード装置2との間のデータの転送を暗号化して行う動作モードのことである。キーボード装置2側で暗号モードを使用する旨の応答をすると、キーボード装置2はユーザIDとパスワードの入力待ちとなる。ここで、図3には示されていないが、キーボード装置2で暗号モードを使用しない旨の応答を行った場合には、以下の処理は行われず、キーボード装置2からの符号等の転送は暗号化を行わない通常の処理となる。

【0026】まず、キーボード装置2からユーザIDが入力されたら、このユーザIDは暗号化せずに直接パーソナルコンピュータ本体1に送信される。パーソナルコンピュータ本体1では、これにより、ユーザ登録の確認が行われる。次に、キーボード装置2の使用者を認証す

るために、パーソナルコンピュータ本体1側から乱数をキーボード装置2に送出する。キーボード装置2ではユーザの入力したパスワードとパーソナルコンピュータ本体1から送信されてきた乱数から所定の算法（例えば、MD5）により圧縮したメッセージをパーソナルコンピュータ本体1に送出する。パーソナルコンピュータ本体1側では、キーボード装置2から送信されてきたメッセージ圧縮されたパスワードと、パーソナルコンピュータ本体1内部に記録されているパスワードを同じ乱数を用いて同じ方法（ここでは、MD5）で圧縮したパスワードとを圧縮されたままの形で比較し、一致するか否かを判断する。一致した場合には、このパスワードを入力した利用者が正当な使用者であることが認められたことになる。

【0027】パーソナルコンピュータ本体1側で利用者が正当なものと確認できると、両者間での暗号の設定を行う。この場合、パーソナルコンピュータ本体1からキーボード装置2に送られるデータとキーボード装置2からパーソナルコンピュータ本体1に送られるデータの両方を暗号化することが考えられる。しかし、実際には、キーボード装置2からパーソナルコンピュータ本体1に送出されるデータが保護されれば十分であるので以下のような処理とする。

【0028】まず、パーソナルコンピュータ本体1から公開鍵とモジュロの除数をキーボード装置2に送出する。キーボード装置2はこの公開鍵とモジュロの除数より、暗号モードでの符号送信に使用するDES暗号鍵をパーソナルコンピュータ本体1に送出する。パーソナルコンピュータ本体1では、暗号化されたDES鍵を復号する。そして、以後、キーボード装置2から送出されるデータは、このDES鍵により暗号化されたデータを使用する。キーボード装置2は、パーソナルコンピュータ本体1に送信するデータをDES鍵で暗号化しながら送信し、パーソナルコンピュータ本体1は、送信されてくる暗号化されたデータをDES鍵で復号しながらパーソナルコンピュータ本体1のホストプロセッサ4に供給する。

【0029】なお、上記一連の処理は、パーソナルコンピュータ本体1のキーボード対応プロセッサ5、暗号化／復号化回路6、及びキーボード装置2のキーボード用プロセッサ7、暗号化回路10によって行われる。

【0030】図4は、キーボード装置側の一連の処理を示した図である。まず、パーソナルコンピュータ本体1で電源が入れると、パーソナルコンピュータ本体1にケーブル3で接続されたキーボード装置2にも電源が投入される（ステップS1）。電源が投入されると、キーボード装置2のキーボード用プロセッサ7はキー8から暗号モードを設定する指示が来ているか否かの判断を行う（ステップS2）。キー8から暗号モードを設定する指示がない場合には、ステップS12に進み、通常モ

ードによって、キーボード装置2から入力されるデータを暗号化せずにパーソナルコンピュータ本体1に送出する。

【0031】ステップS2で、キー8から暗号モードを設定する指示があった場合には、キーボード用プロセッサ7がキーボード装置2をユーザID及びパスワードの入力待ち状態にする。このとき、ユーザID及びパスワードの入力待ち状態をランプ9を点滅することによって表示する。

【0032】なお、パスワードを盗む方法として、アプリケーションプログラムのレベルで、あたかも初期パスワードの入力モードであるかのように、ユーザに錯誤を起こさせる手法が用いられることがある。これを防止するためには画面上の指示と同時にキーボード装置2側の表示も同時に行い、しかもこの状態がアプリケーションでは容易に実現できないようにすることが有効である。通常キーボード装置2には次の3個の表示ランプ9がついている。「大文字入力モード表示」、「スクロールしないモード表示」、「数字入力表示」である。これらのランプ9は、パーソナルコンピュータ本体1側からの指示を受けてキーボード装置2内のキーボード用プロセッサ7が点灯、滅灯を行う。これを通常とは明らかに違う（例えば、特定の周期で全灯が点滅を行う）状態にすることで、パスワードの投入が必要な状態にあることを知らせる（このとき、パーソナルコンピュータ本体1の表示画面には、パスワードの投入が必要な状態にある旨の指示が表示される）。

【0033】この特定の点滅指示が暗号化モード以外の場合に発生しないようにするには、キーボード装置2側で各ランプ9のランプ点滅指示があった場合には同時になく、僅かな時間（0.5秒ほど）ずらして実行するようにし、動作モード切り換えのコマンドに対してのみ完全に同時に点滅するようにすることで実現できる。

【0034】ステップS3でユーザID及びパスワード入力待ち状態に入ると、ユーザからユーザIDが入力されるのを待つ。ユーザIDが入力されると、ステップS4でユーザIDをキーボード装置2からパーソナルコンピュータ本体1へ送信する。パーソナルコンピュータ本体1にユーザIDを送信すると、次に、乱数がパーソナルコンピュータ本体1から送信されてくるので、ステップS5で乱数を受信する。

【0035】すると、次に、パスワード入力待ちとなり、ユーザからのパスワードの入力を待つ。ユーザからパスワードが入力されると、キーボード装置2のキーボード用プロセッサ7は、この送信されてきた乱数を用いてパスワードをMD5でメッセージ圧縮し、パーソナルコンピュータ本体1に送信する（ステップS6）。パーソナルコンピュータ本体1側では、メッセージ圧縮されたパスワードを受け取ると、自身内部に保持しているパスワードを同じ乱数を使ってMD5でメッセージ圧縮し

たものと比較し、一致するか否かの判定結果をキーボード装置2に送信する。

【0036】キーボード装置2側では、パーソナルコンピュータ本体1からユーザIDとパスワードの一致が確認された旨の通知が来たかいないかが判断され（ステップS7）、一致していない旨の通知を受け取った場合には、ステップS3に戻って、再びユーザからのユーザIDとパスワードの入力待ちとなる。このとき、パーソナルコンピュータ本体1の表示には、入力されたユーザIDとパスワードではユーザの認証が行えなかった旨の表示を行うようにする。

【0037】ステップS7で、パーソナルコンピュータ本体1からユーザの認証が成功した旨の通知を受けた場合には、次にパーソナルコンピュータ本体1からDESの暗号鍵をキーボード装置2から送信するための公開鍵が暗号化／復号化回路6で生成されて送られてくるので、これを受信する（ステップS8）。キーボード装置7では、暗号化回路10がこの公開鍵を使って、後のセッション（キーボード装置2からパーソナルコンピュータ本体1へ暗号化した符号を送信する一連の処理）に使われる暗号鍵を暗号化し、キーボード用プロセッサ7を介してパーソナルコンピュータ本体1へ送信する。

【0038】キーボード装置2では、キーボード用プロセッサ7が乱数を発生し、これによりDESの暗号鍵を作成し、パーソナルコンピュータ本体1から送信されてきた公開鍵で暗号化してパーソナルコンピュータ本体1に送信する。パーソナルコンピュータ本体1では、このDESの暗号鍵を復号して暗号化／復号化回路6に設定する。以上により、パーソナルコンピュータ本体1の暗号化／復号化回路6とキーボード装置2の暗号化回路10には、DESの暗号化鍵が設定されるので、以降のデータは、このDESの暗号鍵を使ってパーソナルコンピュータ本体1にキーボード装置2から暗号化されたデータが送信される（ステップS10）。

【0039】ユーザIDとパスワードを用いたパーソナルコンピュータ本体1への入力セッションが終了した場合には、キーボード装置2から何らかの符号を送信するようにする。ステップS11では、セッションを終了する旨の指示がキーボード装置2から入力された場合に、ステップS3に戻って次のセッションを行うため、再び、ユーザIDとパスワードの入力待ちとなる。ステップS11でセッションの終了が指示されない場合には、ステップS10とステップS11の処理を繰り返して、暗号化されたキー入力をパーソナルコンピュータ本体1に送信する処理を繰り返す。

【0040】本実施形態においては、キーボード装置2からパーソナルコンピュータ本体1にパスワードを送る場合、パーソナルコンピュータ本体1側からの乱数を用いて暗号化を行っている。一般に、暗号化に際して暗号・復号鍵が必要になるが、この鍵の配送を更に保護する

ことが必然的に発生する。従って、この乱数の鍵を予めパーソナルコンピュータ本体1とキーボード装置2の間で取り決めてキーボード内のROM等に配置することにより実現することが考えられるが、これでは、キーボードは特注品になり、コストもかかる上にキーボードの管理などのコストもかかり、広く一般に利用することは困難となる。

【0041】従って、本実施形態では、この問題をメッセージ圧縮技術を用いることで解決する。これは同じく乱数を用いるが、この乱数をもとにしてパスワード等の文を一定ルールで変換する方式である。この結果は1:Nの対応となり（原文に対し、圧縮された変換文を復元した際の復元データの候補がN個対応することになり）、乱数と変換文との両者を入力しても原文（ここではパスワード）を推定することが困難なことを利用する。本体側では正解（パスワード）を知っているので自分で作成したメッセージ圧縮の結果と送られてきたものが、一致すればそのパスワードを入力したユーザを資格者と推定出来るが、これを盗聴している人にはパーソナルコンピュータ本体1及びキーボード装置2の両者の送信するデータを相当量入手しない限り、パスワードの入手が困難である。当然ながら十分なデータが入手出来れば計算等により解読は可能なので、一定期間毎にパスワードを変更することは利用者の責任で行わなければならない。

【0042】これと、パーソナルコンピュータ本体1とキーボード装置2の間での公開鍵によるデータの暗号化を併用することで、本実施形態においては完全に汎用性のある（量産可能で、どのシステムにも利用可能な）安全なキーボード装置の提供を可能としている。

【0043】なお、保護を完全なものとするために、データは例えば56ビットのパケットで送出し、その中の有意なデータの位置はオフセット値を先行データに入れるなどの方法により判定が困難にすることが有効である。キーボード装置2は、パーソナルコンピュータ本体1から送信されてくる公開鍵を用いてDESの鍵をホストコンピュータに送出する。この際に例えば、キーボードの入れ換えなどの不正が行われないようにするために送出データに加えて、再度先のパスワードを用いた圧縮メッセージを付加して送出することが望ましい。

【0044】図5は、本実施形態でキーボード装置からパーソナルコンピュータ本体に送信されるデータの構成を説明する図である。キーボード装置2からは有意な情報はキー8を押下したり、離したりしたときにのみ生じる。しかし、このままではキー操作の情報（例えば、入力文字列の長さ等）が容易に漏洩してしまう。これを防止するために、有意なデータがある場合にも無い場合にも同様にキーボード装置2からの信号を送出する。すなわち、キー8が押下されたり、離すことによって生じる有意な情報以外に、ダミー情報を生成してパーソナルコ

ンピュータ本体1に送出するようにする。

【0045】図5（a）は、暗号化された56ビットのデータがキーボード装置2からパーソナルコンピュータ本体1に対して送出されている様子を模式的に描いた図である。

【0046】このように、キーボード装置2からはキー8の押下等の有意なデータの生成とは関係なく、所定の間隔で暗号化されたデータをパーソナルコンピュータ本体1に送出する様にする。各暗号化データは内部に有意なデータを持っているか否かの情報を備えるように構成し、パーソナルコンピュータ本体1側でデータを復元した際に、この情報から送信されてきたデータ内に有意なデータが含まれているか否かを判断できるようにする。そして、有意なデータが含まれている場合のみに所定の位置に含まれている有意なデータを取得して、キーボード装置2からパーソナルコンピュータ本体1への入力データとして取り込む。

【0047】図5（b）は、図5（a）の56ビットの各暗号化データの暗号化前あるいは復号化後のデータの構成を示す図である。暗号化前のデータには、キー8の押下に伴う有意なデータあるいは、キー8の押下等の操作が全く無い状態で生成された無意のデータが9ビット長で含まれている。この9ビットのデータの前には、この9ビットのデータが有意なものか否かを示す1ビットのフラグが設けられる。例えば、この1ビットのフラグが“1”である場合には、次に続くデータは有意なものであることを示し、このフラグが“0”である場合には、次に続くデータは有意なものではないことを示すようにする。従って、56ビットの暗号化データを復号したパーソナルコンピュータ本体1では、このフラグを見て、“1”であれば次のデータは有意であるのでデータを取り込み、フラグが“0”であれば次のデータは有意ではないので取り込まないという処理を行うようにする。

【0048】また、図5（b）の暗号化前あるいは復号化後のデータの例では、ダミービットを前後に付加している。これにより、盗聴した者は、たとえ暗号化データを復元することが出来たとしても、どこに意味のあるデータが配置されているのかが分からない。このような構成のデータでは有意のデータを認識可能であるべきパーソナルコンピュータ本体1側でも、どこに有意なデータが含まれているのかが分からなくなってしまう。そこで、次に送信されてくるブロックの9ビットのデータが復号化後のデータの中でどの位置から開始するかを示すデータを9ビットのデータの後ろの位置に配置するようにする。これにより、次に送信されてくる暗号化データのブロックを復号した場合に、フラグ等の意味のあるデータが配置されている場所を見出すことができるので、暗号化データのブロックを生成する際、フラグ等のデータの存在位置を変えることが出来る。これにより、盗聴



されても、盗聴した者は9ビットのデータがどこにあるのかが容易には分からないので、より機密保持機能を向上することができる。

【0049】このように、暗号モードでの送信中は上りデータはキーボード用プロセッサ7からの送出位置で乱数などの追加を行い、キーの押下の有無にかかわらず定期的に何らかのデータを流し続けることで、入力内容の推定を困難にすることができる。こうして生成されたデータをキーボード装置2の暗号化回路10でDESにより暗号化してパーソナルコンピュータ本体1に送信する。

【0050】図6は、本発明のキーボード装置の第2の実施形態の構成図である。図6において、図1と同じ構成は同じ参照番号が付されており、説明を省略する。本実施形態においては、キー8からの入力を暗号化回路10で暗号化するとともに、光送受信機64によって光信号に変換して、パーソナルコンピュータ本体61に送信する。パーソナルコンピュータ本体61にも光送受信機63が設けられており、キーボード装置2からの信号を受け取るとともに、パーソナルコンピュータ本体61からキーボード装置62へのデータの転送も光信号を使うことによって行う。これらの光信号は光ケーブル65によって転送される。

【0051】本実施形態においては、光ケーブル65の他に電氣的な信号をケーブル66によって授受するように構成されている。ケーブル66はパスワード等盗聴されては困るデータ以外のデータ、例えば、ランプ9を点灯させるためのデータや、クロック、電源等をキーボード装置62に供給するために設けられている。光ケーブル65とケーブル66は、別々に設けて、それぞれをパーソナルコンピュータ本体61に接続するように構成してもよいが、1本のケーブルにまとめて、光接続と電気接続とを1つのコネクタで行えるようにするのが好ましい。

【0052】光信号は電気信号と異なり、ケーブルを伝搬するとき周囲に誘導電磁場を作らないので、電気信号のように容易に盗聴されることがない。従って、第1の実施形態で述べたような暗号化処理と共に、光信号を使ってパーソナルコンピュータ本体61とキーボード装置62の間でパスワードやキー8の押下に対応する符号を送信することにより、盗聴される可能性をかなり小さくすることができる。

【0053】このように、ユーザID、パスワード、キー8による入力符号を暗号化すると共に、光信号として

授受するようにすることにより、盗聴を防ぐことが出来、更に、機密保持機能の高いキーボード装置を提供することができる。

【0054】なお、上記実施形態の説明では、コンピュータの本体はパーソナルコンピュータであることを前提に説明したが、本発明はこれに限られるものではなく、コンピュータ本体とキーボード装置とが分離されており、ケーブルで接続されるような構造を有するコンピュータシステムであれば、どのような構成にも適用することができる。

【0055】

【発明の効果】本発明によれば、例えば、ホテルや公共の場所に設置されたパーソナルコンピュータに外部からのアクセスによる入力データの盗聴や改ざんを困難に出来、安全な運用が可能になる。

【図面の簡単な説明】

【図1】本発明のキーボード装置の第1の実施形態の構成を示す図である。

【図2】本実施形態のキーボード装置の構成の一例を示す図である。

【図3】本実施形態の一連の処理フローを表すタイムチャートである。

【図4】キーボード装置側の一連の処理を示した図である。

【図5】本実施形態でキーボード装置からパーソナルコンピュータ本体に送信されるデータの構成を説明する図である。

【図6】本発明のキーボード装置の第2の実施形態の構成図である。

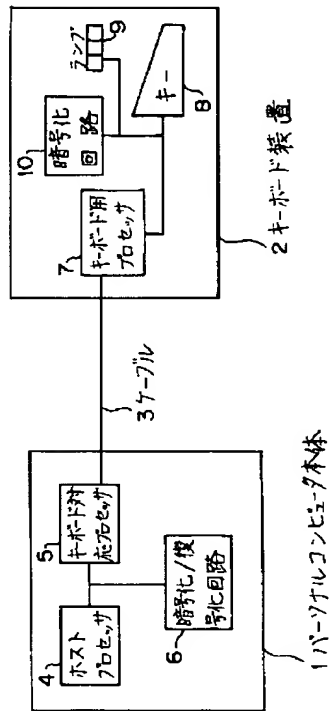
【図7】従来のキーボード装置及びパーソナルコンピュータ本体の構成の一例を示す図である。

【符号の説明】

- |       |               |
|-------|---------------|
| 1、61  | パーソナルコンピュータ本体 |
| 2、62  | キーボード装置       |
| 3、66  | ケーブル          |
| 4     | ホストプロセッサ      |
| 5     | キーボード対応プロセッサ  |
| 6     | 暗号化／復号化回路     |
| 7     | キーボード用プロセッサ   |
| 8     | キー            |
| 9     | ランプ           |
| 10    | 暗号化回路         |
| 65    | 光ケーブル         |
| 63、64 | 光送受信機         |

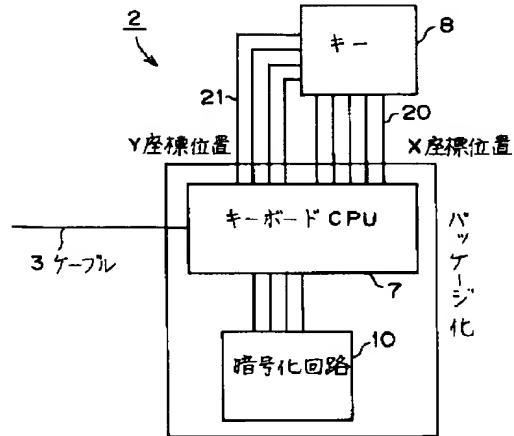
【図1】

本発明のキーボード装置の第1の実施形態の構成を示す図



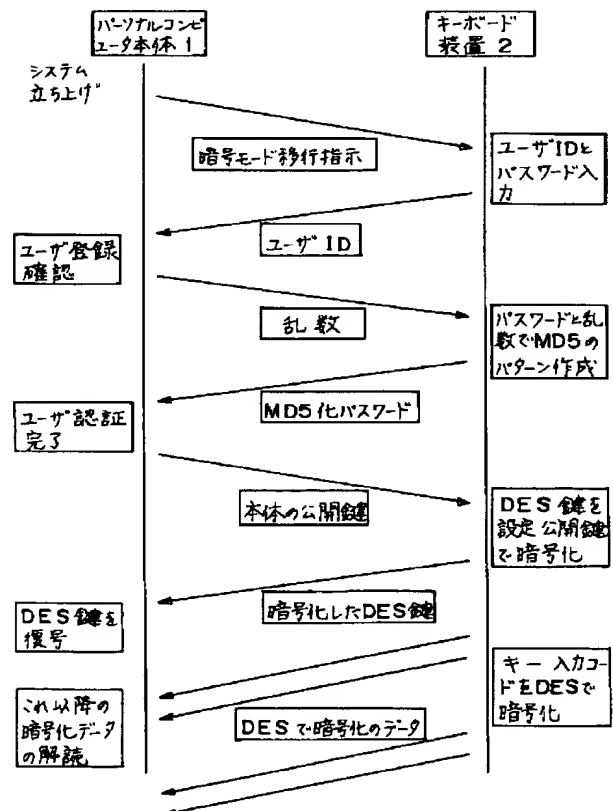
【図2】

本実施形態のキーボード装置の構成の一例を示す図



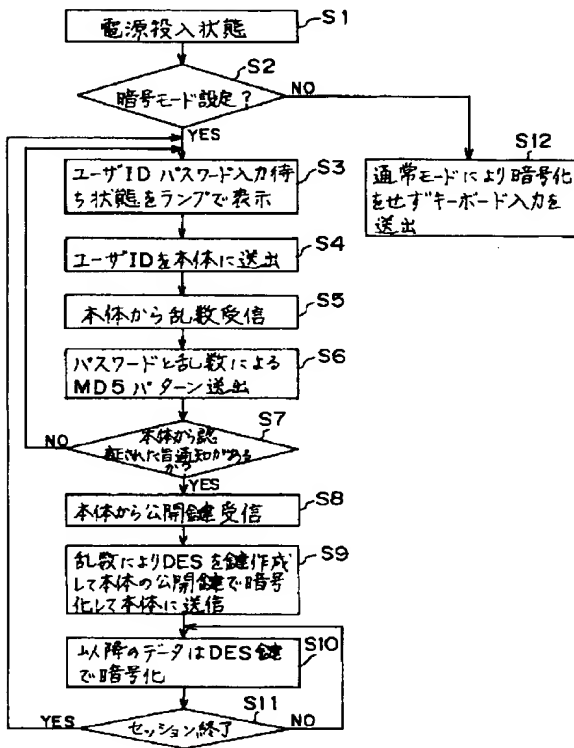
【図3】

本実施形態の一連の処理フローを表すタイムチャート

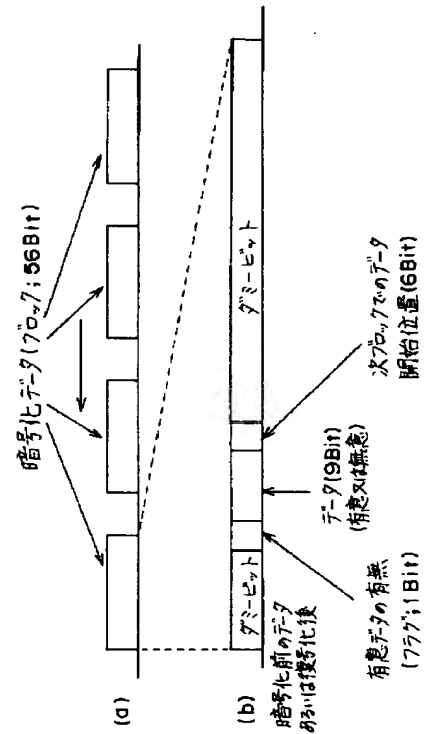


【図4】

キーボード装置側の一連の処理を示した図

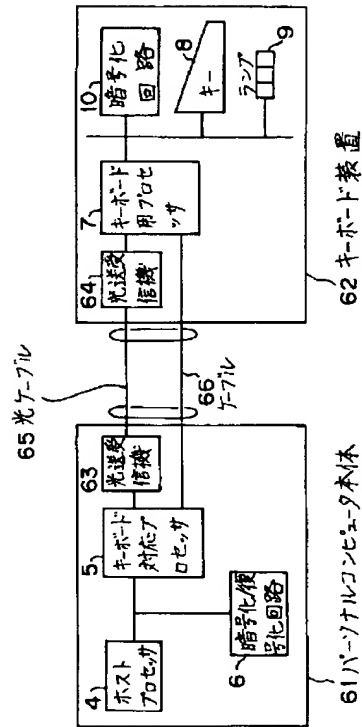


【図5】

本実施形態でキーボード装置からパーソナルコンピュータ  
本体に送信されるデータの構成を説明する図

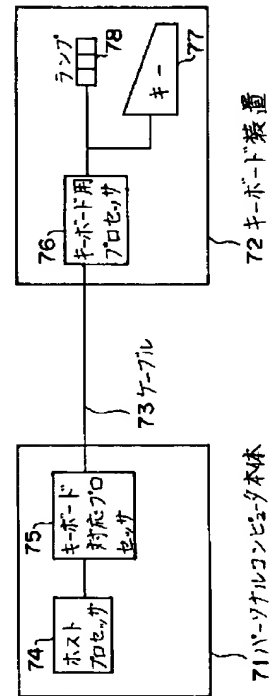
【図6】

本発明のキーボード装置の第2の実施形態  
の構成図



【図7】

従来のキーボード装置及びパーソナルコンピュータ  
本体の構成の一例を示す図



フロントページの続き

(51) Int. Cl.<sup>6</sup>

H04L 9/36

識別記号

F I

H04L 9/00

673C

673A

685